

1 Modulo- und Kongruenzenrechnung

1.1 Einführung

Definition. Seien $n, a, q, r \in \mathbb{Z}$ und $n = aq + r$. Dann schreibt man $n \equiv r \pmod{q}$.

n und r sind also ganze Zahlen, die bei Division durch q den gleichen Rest lassen. Für die meisten Aufgaben ist es günstig, das kleinstmögliche $r \in \mathbb{N}$ (beziehungsweise das größtmögliche $r \in \mathbb{Z}^-$) zu verwenden.

Satz. Es sei $n_1 \equiv r_1 \pmod{q}$ und $n_2 \equiv r_2 \pmod{q}$. Dann gilt auch $n_1 + n_2 \equiv r_1 + r_2 \pmod{q}$.

Es ist $n_1 = p_1q + r_1$ und $n_2 = p_2q + r_2$ mit $p_1, p_2, n_1, n_2, r_1, r_2, q \in \mathbb{Z}$. Dann ist $n_1 + n_2 = p_1q + r_1 + p_2q + r_2 = q(p_1 + p_2) + r_1 + r_2$.

Satz. Es sei $n_1 \equiv r_1 \pmod{q}$ und $n_2 \equiv r_2 \pmod{q}$. Dann gilt auch $n_1n_2 \equiv r_1r_2 \pmod{q}$.

Es ist $n_1 = p_1q + r_1$ und $n_2 = p_2q + r_2$ mit $p_1, p_2, n_1, n_2, r_1, r_2, q \in \mathbb{Z}$. Dann ist $n_1n_2 = (p_1q + r_1)(p_2q + r_2) = p_1p_2q^2 + p_1qr_2 + r_1p_2q + r_1r_2 = q(p_1p_2q + p_1r_2 + r_1p_2) + r_1r_2$.

Mit diesen Sätzen lässt sich folgende Aufgabe lösen:

Aufgabe. Beweise $45 \mid 21^{39} + 39^{21}$.

Wir werden zuerst die Teilbarkeit durch 5 und dann die Teilbarkeit durch 9 zeigen. Weil 5 und 9 teilerfremd sind, ist dies für den Beweis der Teilbarkeit durch 45 hinreichend.

$$\begin{aligned} 21 &\equiv 1 \pmod{5} \Rightarrow 21^{39} \equiv 1^{39} \equiv 1 \pmod{5} \\ 39 &\equiv 4 \equiv -1 \pmod{5} \Rightarrow 39^{21} \equiv (-1)^{21} \equiv -1 \pmod{5} \\ &\Rightarrow 21^{39} + 39^{21} \equiv 1 + (-1) = 0 \pmod{5} \end{aligned}$$

$$21^{39} + 39^{21} = (3 \cdot 7)^{39} + (3 \cdot 13)^{21} = 9 \cdot 3^{37} \cdot 7^{39} + 9 \cdot 3^{19} \cdot 13^{21} = 9 \cdot (3^{37} \cdot 7^{39} + 3^{19} \cdot 13^{21}) \equiv 0 \pmod{9}.$$

1.2 Aufgaben I

1. Beweise: Jede ungerade Quadratzahl ergibt bei Division durch 8 den Rest 1.
2. Überprüfe, ob die Summe zweier ungerader Quadratzahlen wieder eine Quadratzahl sein kann.
3. Wie lauten die beiden letzten Ziffern von 7^{2002} ?

1.3 Lösungen I

1. Eine ungerade Quadratzahl $n^2 \in \mathbb{N}$ ist immer das Quadrat einer ungeraden Zahl $n \in \mathbb{N}$. Nun gilt wegen $\frac{n}{2} \notin \mathbb{N}$ $n \equiv 1 \mod 8 \vee n \equiv 3 \mod 8 \vee n \equiv 5 \mod 8 \vee n \equiv 7 \mod 8$.

Fall 1: $n \equiv 1 \mod 8 \Rightarrow n^2 \equiv 1^2 \mod 8 \Rightarrow n^2 \equiv 1 \mod 8$

Fall 2: $n \equiv 3 \mod 8 \Rightarrow n^2 \equiv 3^2 \mod 8 \Rightarrow n^2 \equiv 1 \mod 8$

Fall 3: $n \equiv 5 \mod 8 \Rightarrow n^2 \equiv 5^2 \mod 8 \Rightarrow n^2 \equiv 1 \mod 8$

Fall 4: $n \equiv 7 \mod 8 \Rightarrow n^2 \equiv 7^2 \mod 8 \Rightarrow n^2 \equiv 1 \mod 8$

2. Nach Aufgabe 1 ist eine ungerade Quadratzahl $n^2 \in \mathbb{N}$ immer kongruent $1 \mod 8$. Man bezeichne nun die beiden ungeraden Quadratzahlen mit q_1 und q_2 .

$$q_1 \equiv 1 \mod 8 \wedge q_2 \equiv 1 \mod 8 \implies q_1 + q_2 \equiv 2 \mod 8$$

$q_1 + q_2$ ist also gerade, aber nicht durch 4 teilbar, was eine gerade Quadratzahl aber sein müsste. Folglich kann die Summe von zwei ungeraden Quadratzahlen nicht wieder eine Quadratzahl sein.

3. Man betrachte die Reste von 7^n beim Dividieren durch 100:

$$7^1 \equiv 7 \mod 100$$

$$7^2 \equiv 49 \mod 100$$

$$7^3 \equiv 343 \equiv 43 \mod 100$$

$$7^4 \equiv 2401 \equiv 1 \mod 100$$

Die Potenzen von 7 sind also modulo 100 periodisch mit Periode 4. Allgemein:

$$\begin{aligned}n \equiv 1 \mod 4 &\implies 7^n \equiv 7 \mod 100 \\n \equiv 2 \mod 4 &\implies 7^n \equiv 49 \mod 100 \\n \equiv 3 \mod 4 &\implies 7^n \equiv 43 \mod 100 \\n \equiv 0 \mod 4 &\implies 7^n \equiv 1 \mod 100\end{aligned}$$

Wegen $2002 \equiv 2 \mod 4$ folgt also $7^{2002} \equiv 49 \mod 100$. Die letzten beiden Ziffern von 7^{2002} sind also 49.

Literatur

- [1] Arthur Engel, Problem Solving Strategies, Springer New York
- [2] Peter Bundschuh, Einführung in die Zahlentheorie, Springer Berlin